REMARKS

Claims 1-17 are pending in the application.

I. REJECTION OF CLAIMS UNDER 35 USC § 103

Claims 1-17 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 6,675153 to Cook in view of US Patent 7,020,638 to Yacobi.

Claims 1, 2, and 7 have been amended herein to correct an antecedent basis issue and correct an instance of use of inconsistent language between claims 1 and 2. No substantive amendments have been made and the applicant respectfully traverses the rejection for at least the following reasons.

Claim 1

The Examiner cites Cook, column 1, lines 24-41 as disclosing a digest created by performing a hash on an electronic fund transfer disbursement file. The applicant respectfully asserts that Cook, Column 1, lines 24-41 do not at all relate to performing a hash function or generating a digest of an electronic fund transfer disbursement file. For convenience, Column 1, lines 24-41 are reproduced in the following paragraph.

> **However, once under the control of a merchant Web site, this personal data can be sold, rented, or otherwise used for commercial gain. Further, the storage and handling of this sensitive data by computer personnel at the merchant site may lead to unauthorized distribution of the data. Internet merchant sites are targets for hackers who may be able to obtain access to this data. In certain instances, accidental release of the data has been made by errors in the software programs that operate a given Web site. A purchaser who has had personal or charge card information compromised may**

then be the victim of unauthorized use of their charge cards or, in more severe cases, complete theft of their identity.

Another problem is the fraudulent use of charge cards. Since it is difficult to determine the identity of a remote purchaser, particularly as it relates to ownership of a given charge card, fraudulent charge card use has become popular on the Internet.

Further, applicants claim 1 includes:

a web server system for transferring authorization control code to the remote system, the authorization control code driving the remote system to perform the following steps:

obtaining the digital signature of authenticated attributes, the authenticated attributes including the digest; and

generating the authorization response, the authorization response including the digital signature.

The Examiner indicates that Cook discloses such limitations of the applicant's invention because cook includes a web server system (the Examiner cites Figure 4) which is well known to do those kind of operations. The Examiner cites columns 2, lines 38-52 for both steps of obtaining a digital signature and generating an authorization response.

First, Column 2, lines 38-52 recites certain steps performed by Cook's ZIXCharge system. There is no teaching that any of such steps are performed by a remote system being driven to do those steps by authorization control code provided by a web server. In fact, it is implied by the totality of the teachings of Cook that the ZIXCharge approval service steps are part of the programming of the ZIXCharge system itself – a teaching that is opposite of a remote system being driven to perform such steps by authorization control code provided by a web server.

Second, one of the steps which the authorization control code drives the remote system to perform is a step of obtaining a digital signature of authenticated attributes – which includes the digest (Note, the applicant's claim indicates that the digest was created by performing a hash on the electronic transfer system and such digest is transferred to the remote system).

Cook includes no teaching or suggestion of generating a digest by hashing an electronic fund transfer disbursement file and sending such digest to a remote system for digital signature.

Thirdly, the second of the steps which the authorization control code drives the remote system perform is to generate the authorization response for transmission back to the system, the authorization response includes the digital signature. While Cook columns 2, lines 38-52 discuss that Cook's ZIXCharge system, upon receiving approval, sends the authorization information back to ZAPI at the merchant web site. There is no teaching of such authorization response which includes the digital signature of the authentication attributes (which specifically includes the digest).

The Examiner acknowledges that Cook does not teach an electronic fund transfer submission module transferring an electronic funds submission to the payment processor – wherein the electronic funds submission comprises the payment transaction file and a least a portion the authorization response comprising a digital signature. It should be noted that in accordance with the applicant's claim the authorization response, with the digital signature, is received from the remote system.

The Examiner indicates that such transfer is taught by Yacobi C1, lines 24-44, C5, lines 50-57, C16, lines 8-14, and C18 lines 54-67.

The applicant respectfully disagrees. The applicant's claim 1 specifically indicates that the fund submission comprises the payment transaction file and at least a portion the authorization response (which, according to applicant's claim is , is provided by the remote system) that includes the digital signature (which the remote system is driven to generate by the authorization control code provided by

the web server). None of the recited sections of Yacoabi teach such a fund submission nor transfer of such a fund submission to payment processor.

Claim 2

The Examiner cites Cook, Column 1, lines 24-41 as teaching authorization control code further providing for the remote system to generate additional message attributes and combine the additional message attributes with the digest to generate the authenticated attributes.

First, as discussed with respect to claim 1, Cook does not teach a remote system being driven to perform any steps by authorization control code that is provided by a web server. As such, cook does not teach authorization control code further driving the remote system to generate additional message attributes and combine the additional message attributes with the digest to generate the authenticated attributes.

Secondly, Column 1, lines 24-41 (pasted in bold in the discussion of claim 1 for convenience) does not include any discussion of generating additional message attributes and combining the additional message attributes with the digest to generate the authenticated attributes.

Claim 3

The Examiner cites Cook, Column 1, lines 14-49 as teaching authorization control code further driving the remote system to: i) pass a dummy data string to a signing component to obtain a dummy authentication data structure; ii) pass the authenticated attributes to the signing component; combine the digital signature with at least a portion of the dummy authentication data structure; and include the authenticated data structure in the authorization response.

Again, as discussed with respect to claim 1, Cook does not teach a remote system being driven to perform any steps by authorization control code that is provided by a web server. As such, Cook does not teach authorization control

code further driving the remote system to perform the steps recited in applicant's claim 3.

Secondly, Column 1, lines 14-49 (again, see pasted in portion in the discussion of claim 1) do not discuss any steps similar to those recited in applicant's claim 3.

Claim 4

The Examiner cites Cook, Column 1, lines 14-49 as teaching authorization control code further driving the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest.

Again, as discussed with respect to claim 1, Cook does not teach a remote system being driven to perform any steps by authorization control code that is provided by a web server. As such, cook certainly does not teach authorization control code further driving the remote system to perform the steps recited in applicant's claim 3.

Secondly, Column 1, lines 14-49 do not discuss any steps similar to combining a digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest.

Claims 5 and 6

Claims 5 and 6 each depend from claim 4 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons.

Claim 7

The Examiner cites Cook, column 1, lines 14-49 and column 2, lines 39-55 as disclosing: i) means for generating a digest by performing a hash on the electronic fund transfer disbursement file; ii) means for transferring the digest to the remote system; iii) means for receiving an authorization response from the remote

system, the authorization response comprising a digital signature of the authenticated attributes, the authenticated attributes comprising the digest.

The applicant respectfully disagrees. None of such means are discussed at column 1, lines 14-49 nor column 2, lines 39-55 (Again see pasted in section in the discussion of Claim 1).

More particularly, with respect to applicant's limitation "means for generating a digest by performing a hash on the electronic fund transfer disbursement file", and "means for transferring the digest to the remote system" – the applicant respectfully asserts that there is no such teaching. At column 2, line 41 there is a teaching of use of a hash to validate an incoming charge slip. There is no teaching that a digest (resulting from performing a hash on an electronic fund transfer disbursement file) is transferred to a remote system.

With respect to applicant's limitation "means for receiving an authorization response from the remote system, the authorization response comprising a digital signature of authenticated attributes, the authenticated attributes comprising the digest" – the applicant respectfully asserts that there is no such teaching. As discussed, the recited sections include no teaching of sending a digest to a remote system and there is no teaching that any authorization response received back from a remote system includes a digital signature of authenticated attributes – which includes the digest.

The Examiner acknowledges that Cook does not teach the applicant's limitation "means for transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature", however, the Examiner recites Yacobi et al as teaching such limitation at column 3, lines 57-64.

For convenience, Yacobi column 3, lines 57-64 are reproduced in the following paragraph.

The user submits the signed payment request along with the bank-signed withdrawal request to the vendor. The vendor evaluates the signatures of the bank and user and ensures that the coin is properly contained within the stick. If all tests pass, the vendor accepts the first asset as payment. Subsequent to this first asset, the user can pass any additional assets from the stick as payment without digitally signing them.

The applicant respectfully asserts that Yacobi, column 3, lines 57-64 do not at all relate to transferring an electronic funds submission to a payment processor where the electronic funds submission comprises both the payment transaction file and a least a portion of the authorization response (which, as defined in the applicant's claim, is from a remote system) comprising the digital signature (which as defined in the applicant's claim, is a digital signature of at least the digest that was sent to the remote system).

Claim 8 – 12

Claims 8 – 12 each depend from claim 7 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons.

Claim 13

Claim 13 depends from claim 7 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons. Further, Claim 13 recites that the payment management system of claim 7, further includes a web server for passing authorization control code to the remote system. The authorization control code is at least one of executable by the remote system and interpretable by the remote system for driving the remote system to perform two distinctive steps.

Those distinctive steps are: i) generate additional message attributes; ii) combine the additional message attributes with the digest to generate the

authenticated attributes. Wherein, the digital signature comprises a digital signature of a hash of the authenticated attributes.

The Examiner indicates that Cook discloses such limitations of the applicants invention because cook includes a web server system (the Examiner cites Column 1, lines 24-41). The applicant respectfully disagrees, column 1, lines 24-41 do not include any teaching of authorization control code that is at least one of executable by the remote system and interpretable by the remote system for driving the remote system to perform the two distinctive steps recited in the applicant's claim.

Claim 13

Claim 14 depends from claim 13 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons. Further, Claim 14 recites that the authorization control code passed to the remote system (e.g. the authorization control code that is at least one of executable by the remote system and interpretable by the remote system for driving the remote system to perform two distinctive steps) additionally drives the remote system to perform four additional distinctive steps – as recited in the claim. .

Again, Column 1, lines 14-49 do not include any teaching of authorization control code that is at least one of executable by the remote system and interpretable by the remote system for driving the remote system to perform any steps. And, as such, Column 1, lines 14-49 do not teach authorization control code driving the remote system to perform the four additional specifically recited steps.

Claim 15

Claim 15 depends from claim 14 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons. Further, Claim 15 recites that the authorization control code passed to the remote system (e.g. the authorization control code that is at least one of executable by the remote system and interpretable by the remote system for driving the remote system to perform

RECEIVED
CENTRAL FAX CENTER
NOV 2 3 2007

two distinctive steps under claim 13, and four additional steps under claim 14) additionally drives the remote system to perform at least one additional distinctive steps – as recited in the claim 15.

Claim 16 – 17

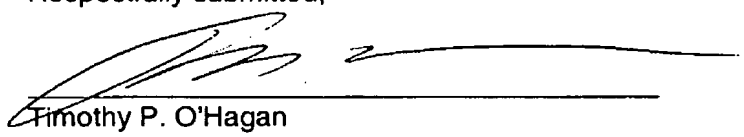
Claims 16-17 each depend from claim 15 and can be distinguished over Cook, Yacobi, and the other art of record for at least the same reasons.

II. CONCLUSION

Accordingly, claims 1-17 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Respectfully submitted,



Timothy P. O'Hagan
Reg. No. 39,319

DATE: 11/23/07

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300